LISTING OF CLAIMS

1-21. (Canceled)

22. (New) An apparatus for producing a pseudo random sequence, comprising:

a data bit generator to produce a principal data stream;

multiple data bit generators to create additional data streams;

a storage structure responsive to the additional data streams having multiple bit storage locations to store the bits of the principal data stream in the storage locations in a pseudo random order based on an order of bits in the additional data streams; and

a shuffle unit coupled with the data bit generators to modify the principal data stream by combining the bits of the principal data stream with past bits of the principal data stream stored in the storage structure and pseudo randomly selected from the storage structure based on an order of the bits in the additional data streams to produce a pseudo random sequence.

23. (New) An apparatus according to claim 22, wherein the data bit generators comprise linear feedback shift registers.

24. (New) An apparatus according to claim 22, wherein the storage unit has a number of addressable bit locations and wherein the additional data streams control write address and read address ports that control access to the number of addressable bit locations.

25. (New) An apparatus according to claim 24, wherein the number of addressable bit locations is a number that has a base 2 relationship with the number of multiple data bit generators.

26. (New) An apparatus according to claim 22, wherein the shuffle unit includes a 1 to n (n an integer greater than 1) de-multiplexer having an input line coupled to the data bit generator

that produces the principal data stream, control lines, at least one of which is coupled to one of the multiple data bit generators, and n output lines coupled to the storage structure.

27. (New) An apparatus according to claim 22, wherein the shuffle unit includes an n to 1 (n an integer greater than 1) multiplexer having n input lines coupled to the storage structure, an output line, and control lines, at least one of which is coupled to one of the multiple data bit generators.

28. (New) An apparatus according to claim 22, wherein the shuffle unit further includes a bit-wise XOR circuit, an input of which receives the bits of the principal data stream and an input of which receives the pseudo randomly selected bits, the output of which is the pseudo random sequence.

29. (New) A method for generating a data stream, comprising:

generating a first and a second bit sequence;

storing bits from the first sequence in a memory structure;

retrieving stored bits of the first sequence from the memory structure in a stochastic order, the order based at least in part on a bit order of the second sequence;

bit-wise modifying the bits of the first sequence with the stochastically retrieved bits to produce a pseudo random data stream.

30. (New) A method according to claim 29, wherein generating the first and second bit sequences comprises generating at least one of the first and the second bit sequences with a linear feedback shift register.

31. (New) A method according to claim 29, wherein storing bits from the first sequence in a memory structure comprises writing to bit-addressable memory locations in the memory structure an address selected output of a 1 to n (n being an integer greater than 1) de-multiplexer,

the input of the multiplexer being the first bit sequence, and the address selection controlled by an order of bits in the second bit sequence.

32. (**New**) A method according to claim 29, wherein retrieving stored bits in the stochastic order from the memory structure comprises retrieving an output of an n to 1 (n being an integer greater than 1) multiplexer, the n address selectable inputs of the multiplexer corresponding to n bit-addressable memory locations in the memory structure, and the address selection controlled by an order of bits in the second bit sequence.

33. (**New**) A method according to claim 29, wherein bit-wise modifying the bits of the first sequence comprises logically XOR-ing the bits of the first bit sequence with the stochastically retrieved bits.

a1

34. (**New**) A method according to claim 29, further comprising generating additional bit sequences, wherein storing and retrieving bits to/from the memory structure comprise storing and retrieving in a stochastic order based on a combined bit order of the second and the additional bit sequences.

35. (**New**) A stream cipher generator comprising:

a first data bit generator to produce a first stream of data bits;

a memory having a read and write port to receive and store bits from the first stream of data bits;

a second data bit generator to produce a second stream of data bits;

a read and write port controller coupled to the memory and responsive to the second stream of data bits, to control the read and write functions of the memory based, at least in part, on the sequence of bits in the second stream of data bits; and

a combiner to receive the first stream of data bits and the bits read from the memory, and modify the first stream of data bits with the bits read from the memory to produce a pseudo random sequence.

36. (New) A stream cipher generator according to claim 35, wherein at least one of the first and the second data bit generators comprise a linear feedback shift register.

37. (New) A stream cipher generator according to claim 35, wherein the memory further includes a bit-addressable address selection port.

38. (New) A stream cipher generator according to claim 37, wherein the read and write port controller further comprises a 1 to n (n being an integer greater than 1) de-multiplexer, the de-multiplexer input coupled to the first data bit generator, the n outputs coupled to n bit locations of the bit-addressable memory, and a control line coupled to the second data bit generator to make the address selection responsive to an order of bits in the second stream of data bits.

39. (New) A stream cipher generator according to claim 37, wherein the read and write port controller further comprises an n to 1 (n being an integer greater than 1) multiplexer, the n multiplexer inputs coupled to n locations of the bit-addressable memory, the multiplexer output coupled to the combiner, and a control line coupled to the second data bit generator to make the address selection responsive to an order of bits in the second stream of data bits.

40. (New) A stream cipher generator according to claim 37, further comprising additional data bit generators, and wherein the read and write port controller controls the read and write functions of the memory based on a sequence of bits of the combination of the second stream of data bits and data streams generated by the additional data bit generators.

41. (New) A stream cipher generator according to claim 35, wherein the combiner comprises a bit-wise XOR circuit to XOR the bits of the first stream of data bits with the bits read from the memory, and the XOR output comprises the pseudo random sequence.